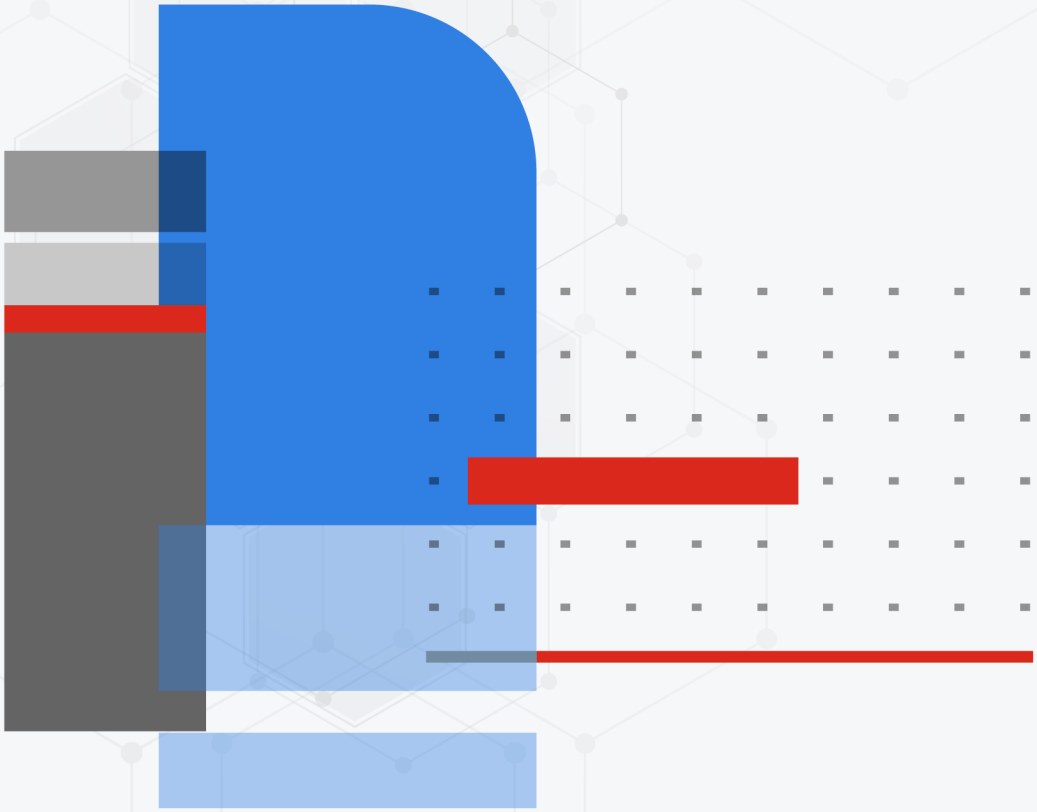
Release Notes

FortiSwitchOS 7.4.1



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

September 28, 2023
FortiSwitchOS 7.4.1 Release Notes
11-741-923196-20230928

TABLE OF CONTENTS

Change log

Date	Change Description
September 21, 2023	Initial release for FortiSwitchOS 7.4.1
September 28, 2023	Updated the description of one of the features in the “What’s new in FortiSwitchOS 7.4.1“ section.

Introduction

This document provides the following information for FortiSwitchOS 7.4.1 build 0787.

See the Fortinet Document Library for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 7.4.1 supports the following models:

FortiSwitch 1xx	FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE
FortiSwitch 2xx	FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE
FortiSwitch 4xx	FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448E, FS-448E-POE, FS-448E-FPOE
FortiSwitch 5xx	FS-524D, FS-524D-FPOE, FS-548D, FS-548D-FPOE
FortiSwitch 1xxx	FS-1024D, FS-1024E, FS-1048E, FS-T1024E
FortiSwitch 3xxx	FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D, FSR-424F-POE

What's new in FortiSwitchOS 7.4.1

Release 7.4.1 provides the following new features:

- The FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148F, FS-148F-POE, and FS-148F-FPOE models now support flow export.
- The FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448E, FS-448E-POE, and FS-448E-FPOE models now support Protocol Independent Multicast (PIM) routing.
- The FS-1024E and FS-T1024E models now support Media Access Control security (MACsec) on 4x25G split ports.
- You can now configure MACsec profiles in the GUI.
- You now have the flexibility to exclude one or more protocols from the MACsec traffic policy. By default, all protocols are encrypted. You can use the CLI to exclude ARP, 802.1q VLAN, FortiLink, IPv4, IPv6, LACP, LLDP, 802.1ad QinQ, and STP packets.
- When strong cryptography is disabled in the *System* > *Config* > *SSL* page, FortiSwitchOS displays a warning that the switch will reboot and then requires the user to confirm before rebooting the switch.
- You can now generate an elliptic curve (ECDSA) certificate using a certificate signing request (CSR). You can choose an SECP256R1, SECP384R1, or SECP521R1 elliptic curve.
- You can use new CLI commands to specify how the following RADIUS request attributes are formatted:
  - User-Name
  - User-Password
  - Called-Station-Id
  - Calling-Station-Id
- You can now configure network monitoring and view network-monitoring statistics in the GUI. You can monitor specific unicast MAC addresses in directed mode, monitor all detected MAC addresses on a FortiSwitch unit in survey mode, or do both.
- You can now configure Intermediate System to Intermediate System Protocol (IS-IS) routing in the GUI.
- FR-TRAN-ZX now supports the diagnostic monitoring interface (DMI).
- FortiSwitchOS can now distinguish between the interchassis link (ICL) being down and a peer switch being down or getting restarted. When a peer switch is down or restarted, the other switch does not mistakenly detect a split-brain state and shut down all ports.
- You can now configure in the CLI how long MAC authentication bypass (MAB) sessions are kept:
  - In static mode, MAB sessions are kept until the link goes down or the MAB sessions are manually deleted with the CLI.
  - In dynamic mode, MAB sessions are treated the same way as dynamically learned MAC addresses.
- You can now use flow-based Equal Cost Multi-Path (ECMP) routing with Virtual Extensible LAN (VXLAN) interfaces for load balancing.
- The `set vxlan-port` command (under `config switch global`) is now the `set vxlan-dport` command.
- FortiSwitchOS can now detect duplicate MAC addresses in a Border Gateway Protocol (BGP) Ethernet Virtual Private Network (EVPN) with VXLAN interfaces. When a duplicate MAC address is detected, FortiSwitchOS logs it as an error, making it quicker to find and resolve problems in the network configuration.
- The FS-1048 model now supports autonegotiation for the 40G direct-attach cable (FN-CABLE-QSFP+).
- If you are using FortiSwitchOS 7.4.1 in FortiLink mode:
  - You can now make your Security Fabric more secure with the FortiLink secured fabric. The FortiLink secured fabric provides authentication and encryption to all fabric links, wherever possible. Zero-touch support is available for FortiLink mode over a layer-2 network and over a layer-3 network.

- Managed FortiSwitch units can now perform inter-VLAN routing. The FortiGate device can program a FortiSwitch unit to do the layer-3 routing of trusted traffic between specific VLANs.

Refer to the FortiSwitch feature matrix for details about the features supported by each FortiSwitch model.

Special notices

Zero-touch management

When a new FortiSwitch unit is started, by default, it will connect to the available manager, which can be a FortiGate device, FortiLAN Cloud, or FortiSwitch Manager. All ports are enabled for auto discovery. The “internal” interface is the DHCP client in all FortiSwitch models. If you do not want your FortiSwitch unit to be managed, you must disable the features that you do not want active.

By default, auto-network is enabled in FortiSwitchOS 7.2.0 and later

After an `execute factoryreset` command is executed on a FortiSwitch unit in standalone mode, the auto-network configuration is enabled by default. If you are not using auto-network, you must manually disable it:

```
config switch auto-network
   set status disable
end
```

Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than 6.2.6 or 6.4.4 is not supported

Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.2.6 and later 6.2 versions is supported. Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.4.4 and later 6.4 versions is supported. Downgrading FortiSwitchOS 7.0.0 to versions earlier than FortiSwitchOS 6.2.6 or 6.4.4 is not supported.

Downgrading your FortiSwitchOS version requires converting the admin password format first

Before downgrading to a FortiSwitchOS version earlier than 7.0.0, you need to ensure that the administrator password is in SHA1 format. Use the `execute system admin account-convert-sha1` command to convert the administrator password to SHA1 encryption.

Before downgrading to FortiSwitchOS 7.0.0 or later, you need to ensure that the administrator password is in SHA1 or SHA256 format.

- Use the `execute system admin account-convert-sha1` command to convert the administrator password to SHA1 encryption.
- Use the `execute system admin account-convert-sha256` command to convert the password for a system administrator account to SHA256 encryption.

If you do not convert the admin password before downgrading, the admin password will not work after the switch reboots with the earlier FortiSwitchOS version.

To convert the format of the admin password to SHA1 format:

1. Enter the following CLI command to convert the admin password to SHA1 encryption:

   ```
   execute system admin account-convert-sha1 <admin_name>
   ```

2. Downgrade your firmware.

To convert the format of the admin password to SHA256 format:

1. Enter the following CLI command to convert the admin password to SHA256 encryption:

   ```
   execute system admin account-convert-sha256 <admin_name>
   ```

2. Downgrade your firmware.

Connecting multiple FSR-112D-POE switches

The FSR-112D-POE switch does not support interconnectivity to other FSR-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

Upgrade information

FortiSwitchOS 7.4.1 supports upgrading from FortiSwitchOS 3.5.0 and later.

For the FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, and FS-M426-FPOE models, there is a two-step upgrade process if you are upgrading from FortiSwitchOS 6.0.x or 6.2.x to 7.2.x:

1. Upgrade from FortiSwitchOS 6.0.x or 6.2.x to FortiSwitchOS 6.4.12 or later.
2. Upgrade from FortiSwitchOS 6.4.12 or later to 7.2.x.

If you do not follow the two-step upgrade process, the FortiSwitch unit will not start after the upgrade, and you will need to use the serial console to conclude the upgrade (BIOS and OS).

For FortiSwitch units managed by FortiGate units, refer to the *FortiLink Release Notes* for upgrade information.

Product integration and support

FortiSwitchOS 7.4.1 support

The following table lists FortiSwitchOS 7.4.1 product integration and support information.

Web browser	• Mozilla Firefox version 52 • Google Chrome version 56 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS (FortiLink Support)	Refer to the FortiLink Compatibility table to find which FortiSwitchOS versions support which FortiOS versions.

Resolved issues

The following issues have been fixed in FortiSwitchOS 7.4.1. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
896925	When `set edge-port` is disabled, “BPDU Guard: Resetting <interface_name>.” is logged during a broadcast storm, even though `set stp-bpdu-guard` is not enabled.
897887	After enabling the blocking of intra-VLAN traffic on the VLAN, the user cannot connect to the internet or ping the gateway address.
910257	Going to *System* > *Config* > *Firmware* causes a “500 Internal Server Error.”
914774	After energy efficient Ethernet is enabled on FS-448E, received packets are no longer processed on ports 33-36.
917919	When the administrator login name is longer than 35 characters, the GUI displays an “Internal Server Error” message.
918017	When RSPAN is enabled on FSR-112D-POE in FortiLink mode, FortiLink goes down, and traffic on FortiLink stops.
919505	MAB authentication fails on FS-148F-FPOE running FortiSwitchOS 7.2.4 for laptops and phones.
919943	When the setting for strong cryptology is changed, the new setting does not take effect until the switch is restarted.
919990	The GUI displays a warning message of “Unverified Image Detected” when the user logs in to FortiSwitchOS 7.4.0 build 0767, even though the image is verified.
921600	The STP state changes when the cable that connects the FortiSwitch port to a PC is unplugged and then plugged in again.
922098	When a device is connected to an FS-148F-FPOE managed by FortiCloud, the network becomes unstable.
922571	When importing a local PKCS12 certificate, the certificate name cannot be longer than 63 characters.
924247	After enabling sticky MAC and the MAC learning limit on FS-1xx models, new MAC addresses are not learned after old MAC entries were cleared from the port.
930931	DHCPv6 packets were seen in the internal port of the FS-124F-FPOE models.
935537	After setting the FS-108F-PoE port to perpetual PoE, the setting did not take effect without restarting the switch.
940956	Adding or removing an SNMP community on a tier-1 MCLAG switch causes the switch to become unresponsive for 10 seconds on all VLANs when a large number of network interfaces are configured.
941692	After DHCP snooping is enabled on FS-1xx models, devices cannot receive DHCP addresses.
942118	After configuring MACsec on the FS-524D model, the switch becomes unresponsive and stops forwarding traffic.

Bug ID	Description
942140	The MAC address moves between FortiAP units when the FortiAP units are connected to two different FortiSwitch units.
942586	Going to *System* > *Config* > *Time* when running FortiSwitchOS causes black stripes to appear in the GUI.
945471	Configuring a low VRRP ID number on one of a pair of FS-T1024E switches causes the switch to lose connection with the backup switch.

Known issues

The following known issues have been identified with FortiSwitchOS 7.4.1. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
382518, 417024, 417073, 417099, 438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANs).
414972	IGMP snooping might not work correctly when used with 802.1x Dynamic VLAN functionality.
480605	When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server **Workarounds:** • Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN. • Temporarily disable DHCP snooping on the VLAN and then use the `execute interface dhcpclient-renew <interface>` command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping.
510943	The time-domain reflectometer (TDR) function (cable diagnostics feature) reports unexpected values. **Workaround:** When using the cable diagnostics feature on a port (with the `diagnose switch physical-ports cable-diag <physical port name>` CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.
542031	For the FS-5xx switches, the `diagnose switch physical-ports led-flash` command flashes only the SFP port LEDs, instead of all the port LEDs.
548783	Some models support setting the mirror destination to “internal.” This is intended only for debugging purposes and might prevent critical protocols from operating on ports being used as mirror sources.
572052	Backup files from FortiSwitchOS 3.x that have 16-character-long passwords fail when restored on FortiSwitchOS 6.x. In FortiSwitchOS 6.x, file backups fail with passwords longer than 15 characters. **Workaround:** Use passwords with a maximum of 15 characters for FortiSwitchOS 3.x and 6.x.
585550	When packet sampling is enabled on an interface, packets that should be dropped by uRPF will be forwarded.
606044/610149	The results are inaccurate when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.

Bug ID	Description
609375	The FortiSwitchOS supports four priority levels (critical, high, medium, and low); however, The SNMP Power Ethernet MIB only supports three levels. To support the MIB, a power priority of medium is returned as low for the PoE MIB.
659487	The FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE, FS-148E, and FS-148E-POE models support ACL packet counters but not byte counters. The `get switch acl counters` commands always show the number of bytes as 0.
667079	For the FSR-112D-POE model: • If you have enabled IGMP snooping or MLD snooping, the FortiSwitch unit does not support IPv6 features and cannot pass IPv6 protocol packets transparently. • If you want to use IGMP snooping or MLD snooping with IPv6 features, you need to enable `set flood-unknown-multicast` under the `config switch global` command.
673433	Some 7-meter direct-attach cables (DACs) cause traffic loss for the FS- 448E model.
748210	The MAC authentication bypass (MAB) sometimes does not work on the FS-424E when a third-party hub is disconnected and then reconnected.
777647	• When MACsec is enabled on a tagged port, the `set exclude-protocol` command does not work on packets with VLAN tags (ARP, IPv4, or IPv6). • If you use the `set exclude-protocol` command with dot1q and packets with VLAN tags (ARP, IPv4, or IPv6), the packets are not MACsec encrypted and are transmitted as plain text. • Only 0x88a8 type packets apply to qinq.
784585	When a dynamic LACP trunk has formed between switches in an MRP ring, the MRP ring cannot be closed. Deleting the dynamic LACP trunk does not fix this issue. MRP supports only physical ports and static trunks; MRP does not support dynamic LACP trunks. **Workaround:** Disable MRP and then re-enable MRP.
793145	VXLAN does not work with the following: • log-mac-event • DHCP snooping • LLDP-assigned VLANs • NAC • Block intra-VLAN traffic
828603	The `oids.html` file is not accurate.
829807	eBGP does not advertise routes to its peer by default unless the `set ebgp-requires-policy disable` command is explicitly configured or inbound/outbound policies are configured.
867108	Depending on your browser type/version, web UI access might fail when using TLS 1.3 and client certificate authentication. **Workaround:** Use TLS 1.2.

Bug ID	Description
903001	Do not use `mgmt` as the name of a switch virtual interface (SVI). `mgmt` is reserved for the physical management switch port.
916405	FortiSwitchOS should not allow MACsec and 802.1X authentication to be configured on the same port.
939257	If you set the `sample-direction` to `tx` or `both`, the output of the `get system flow-export-data flows all` command might be wrong. **Workaround:** Set the `sample-direction` to `rx`.
940248	When both network device detection (`config switch network-monitor settings`) and the switch controller routing offload are enabled, the FS-1048E switch generates duplicate packets.
950895	In Release 7.4.1, VXLAN supports only one MSTP instance.

www.fortinet.com